U.S. Department of Justice

United States Attorney
Eastern District of New York

SDD:MW/SK
F. #2015R00439

271 Cadman Plaza East
Brooklyn, New York 11201

August 9, 2017

By Hand and ECF

The Honorable Nicholas G. Garaufis
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Fabio Gasperini
Criminal Docket No. 16-441 (NGG)

Dear Judge Garaufis:

The government respectfully submits this letter in advance of sentencing in this case, scheduled for August 9, 2017, at 3:00 p.m. On August 4, 2017, a jury in the Eastern District of New York convicted the defendant of one count of computer intrusion in violation of Title 18, United States Code, Section 1030(a)(2). The defendant's count of conviction carries a statutory maximum sentence of one year of imprisonment and a statutory maximum fine of $100,000. See 18 U.S.C. §§ 1030(c)(2)(A), 3571(b)(5). As discussed below, the government respectfully requests that the Court impose the statutory maximum sentence of 12 months' incarceration, a $100,000 fine, a one year term of supervised release, and forfeiture of the defendant's botnet, the defendant's infrastructure used to manage and run the botnet (including computers, command-and-control servers, and domains), and the defendant's backdoor (with username "request").

I. Offense Conduct

Given the Court's familiarity with the case, the government provides the following brief summary of relevant facts for the Court's consideration at sentencing.

The defendant was an information technology professional in Rome, Italy, see GX 2144T, who devised a scheme to attack QNAP servers via the "Shellshock"

vulnerability, a weakness in the source code of Linux-based computers, in order to obtain complete control over the serves, obtain usernames and passwords from the servers, and use the servers to fraudulently inflate traffic to advertisements on the defendant's websites. The defendant used malicious software, e.g., GX 102 (pastebin Shellshock script), 202A (qnap.worm), 1401A (S00.sh script) and 1401B (S0.sh script) to enter the servers without permission. The defendant attacked and attempted to attack servers around the world, including the computer systems of the Port of Los Angeles and the computer systems of the state government of Washoe County, Nevada, which used a QNAP server to facilitate the activities of its crime lab. In doing so, the defendant completely compromised the servers that he successfully attacked, and violated the privacy and security of the individuals and businesses that owned them. See Exhibit A (victim impact statement of Dan Pickering); Exhibit B (victim impact statement of Caroline Shields forthcoming). The defendant's exploitation of the Shellshock vulnerability further victimized the server manufacturer that he targeted, QNAP, which spent significant resources to develop a solution to protect its customers from the Shellshock vulnerability and the hackers who were exploiting it. See Exhibit C (QNAP cost table for developing a fix for the Shellshock vulnerability); GX 13 (QNAP advisory releasing "urgent fix" for the defendant's unauthorized "request" account).

After the defendant used computer viruses to infect QNAP servers, the defendant caused the QNAP servers to download additional files from command-and-control servers he leased from companies in the United States (e.g. Linode, ServerHub, ColoCrossing) and abroad (e.g. UAservers). For example, the ServerHub server, bearing IP address 23.231.6.11, stored the "cl" script, which the defendant used to search for and take ccCam username and password files; it also stored the "emme" script, which the defendant used to cause the infected servers to "view" website advertisements as if they were real human beings. The Linode server, bearing IP address 178.79.183.247, stored the "agent.php" script, which the defendant used to disguise the infected servers as real people with the camouflage of web browsers. Over 150,000 computers worldwide connected to the defendant's command-and-control server at Linode, and over 90,000 computers worldwide requested and downloaded the defendant's agent.php script from the Linode server. E.g. GX 362, 1357. Likewise, the Linode server contained logs showing that over 120,000 computers downloaded the "cl," "cl1," "emme," and "emme1" scripts. GX 1362. The ColoCrossing server, bearing IP address 23.95.112.70, was an Internet Relay Chat ("IRC") server, which the defendant used to communicate with the servers he had infected and give them commands. See GX 901; GX 1323; GX 2045.

The defendant also created a backdoor account on the infected QNAP servers, bearing the username "request," that he could use at his whim. The password for this account was admitted into evidence at trial. See GX 5000. The defendant made use of this backdoor: for example, in November and December 2014, he remotely accessed and logged

into twelve different computers using the username "request." GX 1332. At least three of those computers were confirmed to be QNAP servers that were still operational and in use as of this year. See GX 9-11. After creating this backdoor account, the defendant "patched" the Shellshock vulnerability, locking out other hackers.

One purpose of the defendant's scheme was to effect fake "clicks" on websites owned and operated by the defendant. See e.g., GX 2045 (photograph of the defendant commanding the infected servers to click on an advertisement on one of his websites); GX 2031 ("clicks completed" notification emails); GX 2042 (photograph of defendant tracking fraudulent advertising revenue). From 2011-2016, the defendant was paid 92,607.65 Euros — the equivalent of approximately $121,000 — by JuiceADV, an Italian advertising company defrauded by the defendant. GX 3003G. While each of the websites was owned by the defendant, see GX 1211R, beginning in 2014, the defendant stopped receiving payments directly from JuiceADV for those websites, instead routing payments to eight other people in order to conceal the income generated from those websites and avoid Italian reporting requirements. See GX 3003G; e.g., GX 3009 (payments for a website owned by the defendant going to Anthony Ventura, with username "tonygasp"). PayPal records showed that one of the defendant's co-conspirators, Fabrizio Bagnato, sent the defendant a cut of approximately 50% of the JuiceADV payments that Bagnato received. See GX 5004. In addition, the defendant used other co-conspirators to launder money in cash. One of those co-conspirators, Fabio Fochetti, admitted to Italian law enforcement that he assisted the defendant in concealing the defendant's profits related to his websites. See Exhibit D (statement of Fabio Fochetti and English translation). During the interview, Fochetti stated that he was friends with the defendant and the defendant's fiancée Maria Napoleoni. Toward the end of 2014, Napoleoni told Fochetti that the defendant was publishing advertisements on his websites and needed to "reroute his earnings to someone else, because he had already made $5,000.00 Euros for that year." Id. at 9. Fochetti further stated that Napoleoni asked him if he was willing to "receive the proceeds" from the defendant's websites. Id. at 10. Shortly after, the defendant contacted Fochetti and explained that he published advertisements on his website for a fee and asked Fochetti if he was willing to receive some of the proceeds because the defendant had already earned 5,000 Euros that year. Fochetti agreed and thereafter began receiving payments to his bank account. "Unfailingly" he withdrew cash from his account and gave the full amount to Napoleoni, who then provided it to the defendant. Id.

After his scheme was uncovered, the defendant took affirmative steps to destroy evidence and conceal his criminal activities. After his arrest in the Netherlands, his Facebook account was shut down and emails and other content from his Google accounts were deleted. E.g., GX 1508, 2060A-T. Likewise, when Italian law enforcement searched the defendant's home, the hard drive to the defendant's computer had been thrown away,

despite the fact that several other old hard and broken drives were kept in a closet in the home. Finally, analysis of one of the hard drives recovered from this search, which included a user account under the name "gaspolo," demonstrated that special forensic deletion software had been used to permanently delete files, making it impossible to recover incriminating information from the hard drive. E.g., GX 1351. In ensuring the destruction of this evidence — particularly his computer hard drives — the defendant successfully deprived the jury of additional evidence of the click fraud, as historical photographs of the defendant's computer show that he used it to log in to his botnet's command-and-control servers and store records of his fraudulent clicks. See GX 2041, GX 2042 (click tracking software on home computer); GX 2048, GX 2049 (documents on home computer desktop entitled "click2.txt," "click111.txt," and "randomclick.txt").

II. Legal Standards

In the Supreme Court's opinion in United States v. Booker, 543 U.S. 220, 245 (2005), which held that the Guidelines are advisory not mandatory, the Court made clear that district courts are still "require[d] . . . to consider Guidelines ranges" in determining a sentence, but also may tailor the sentence in light of other statutory concerns. See 18 U.S.C. § 3553(a). Subsequent to Booker, the Second Circuit held that "sentencing judges remain under a duty with respect to the Guidelines . . . to 'consider' them, along with the other factors listed in section 3553(a)." United States v. Crosby, 397 F.3d 103, 111 (2d Cir. 2005).

In Gall v. United States, 552 U.S. 38 (2007), the Supreme Court elucidated the proper procedure and order of consideration for sentencing courts to follow: "[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark." Gall, 552 U.S. at 49 (citation omitted). Next, a sentencing court should "consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party. In so doing, the Court may not presume that the Guidelines range is reasonable. It must make an individualized assessment based on the facts presented." Id. at 49-50 (citation and footnote omitted).

III. Guidelines Calculation

At trial, the defendant was convicted of computer intrusion. Although the defendant was acquitted of other counts of computer intrusion, wire fraud, wire fraud conspiracy and money laundering conspiracy, the facts related to these counts were proven by the government by a preponderance of the evidence at trial and may therefore be considered in calculating the applicable guidelines range.

"In discharging his duty of imposing a proper sentence, the sentencing judge is authorized, if not required, to consider all of the mitigating and aggravating circumstances involved in the crime." Williams v. State of Okla., 358 U.S. 576, 585 (1959). Since an "[a]cquittal d[oes] not have the effect of conclusively establishing the untruth of all the evidence introduced against [a] defendant," United States v. Sweig, 454 F.2d 181, 184 (2d Cir.1972), and since disputed facts for purposes of sentencing need only to be established by a preponderance of the evidence, see, e.g., United States v. Lee, 818 F.2d 1052, 1057 (2d Cir.), cert. denied, 484 U.S. 956 (1987), the sentencing court is entitled to consider information that the defendant had engaged in conduct that was the subject of an acquittal, United States v. Roland, 748 F.2d 1321, 1327 (2d Cir.1984); United States v. Sweig, 454 F.2d at 183. United States v. Concepcion, 983 F.2d 369, 388 (2d Cir. 1992).

Accordingly, the government submits that the following Guidelines calculation applies:

Base Offense Level (§ 2B1.1)	6
Plus: Loss Exceeded $95,000 (§ 2B1.1(b)(1)(E))	+8
Plus: Offense involved 10 or more victims (§ 2B1.1(b)(2)(A))	+2
Plus: Substantial part of the scheme committed from outside the United States and use of sophisticated means (§ 2B1.1(b)(10)(B) and (C))	+2
Plus: Possession and use of authentication feature (§ 2B1.1(b)(11))	+2
Plus: Intent to obtain personal information (§ 2B1.1(b)(17))	+2
Plus: Offense involved computer systems used for critical infrastructure or by a government entity in furtherance of the administration of justice (§ 2B1.1(b)(18)(A)(i))	+2
Plus: Obstruction of justice (§ 3C1.1)	+2
Total:	26

Thus, the defendant's total offense level is 26, which, based on a criminal history category of I, carries an advisory range of imprisonment of 63-78 months' imprisonment.

IV. Analysis

The government respectfully requests that the Court impose the statutory maximum sentence of 12 months' incarceration, a $100,000 fine, a one year term of supervised release, and forfeiture of the defendant's botnet, the defendant's infrastructure used to manage and run the botnet (including computers, command-and-control servers, and domains), and the defendant's backdoor (with username "request").

a. Term of Imprisonment

A sentence of 12 months' imprisonment accounts for the seriousness of the defendant's criminal conduct. Here, the defendant surreptitiously built and maintained a powerful botnet, an army of infected computers, that spanned the globe. The defendant's botnet included more than 100,000 QNAP servers, thousands of which are located in the United States. The defendant used this botnet to defraud advertisers and steal password information. However, the botnet was also set up to permit the use of more serious attacks, including distributed denial of service or "DDos" attacks which are used to flood a network or website with traffic, causing it to shut down, and thereby denying legitimate users access to that site or service. Indeed, the botnet's potential criminal use in the hacking community is reflected in the value of the botnet itself. As established at trial, a botnet can be bought or rented for as little as $1 per infected computer — rendering the defendant's botnet worth more than $100,000 on the online black market.

The sophistication of the defendant's scheme also requires that the statutory maximum sentence be imposed. Here, the defendant adapted and created malicious software to accomplish his fraudulent goals, including the theft of authentication features such as ccCam usernames and passwords. He also took steps to conceal his criminal tools and evade detection by storing and deploying those malware scripts from various rented servers in the U.S. and abroad. In addition, the creation of the secret "request" user account, permitting the defendant unlimited — and effectively permanent — access to the infected devices, gave the defendant's scheme long-term viability and ensured that he could use his botnet for new and different criminal purposes as time went on. This is especially serious given the evidence that the botnet had the ability to launch "DDoS" attacks, the defendant's ownership and use of password cracking software, and the defendant's ownership and use of scanning software designed to search the internet for vulnerable computers for future attack.

The defendant's concealment of his criminal conduct extended to his deletion of evidence, including the deletion of Facebook and Google records, the destruction of his computer hard drive and the use of forensic deletion software on one of the recovered hard drives. It also extended to the defendant's use of co-conspirators to launder money. As

discussed above, the money laundering activity included routing payments to nine different individuals, including Antonio Ventura, Fabrizio Bagnato, and Fabio Fochetti.

Finally, a 12-month sentence reflects the history and characteristics of the defendant, including his training and experience as an IT professional in Italy, which he used to further his criminal scheme.

b. Imposition of a Fine

The government also respectfully requests that the Court impose a fine of $100,000 on the defendant. Title 18, United States Code, Section 3571 provides that a fine of up to $100,000 may be imposed where an individual has been convicted of a Class A misdemeanor. U.S.S.G. Section 5E1.2 further provides a fine range of $25,000 - $250,000 for defendants assigned offense level 26. Here, the imposition of a $100,000 fine would promote respect for the law, provide just punishment and afford additional specific and general deterrence. The amount is also commensurate with the defendant's earnings from JuiceADV, the value of his botnet if rented or sold on the black market, and the cost of the greater than 100,000 infected computers that the defendant had at his disposal if he had rented that number of servers from companies like Linode, etc. in the United States.

c. Supervised Release

The government also respectfully requests that the Court impose a one year term of supervised release. Title 18, United States Code, Section 3583(b)(3) permits the Court to order up to one year of supervised release for the count of conviction. Ordinarily, for individuals who are deportable aliens, such as the defendant, a term of supervised release is unnecessary. However, U.S.S.G. Section 5D1.1(c) Application Note 5 provides that the Court "should, however, consider imposing a term of supervised release on such a defendant if the [C]ourt determines it would provide an added measure of deterrence and protection based on the facts and circumstances of a particular case." In light of the seriousness of the defendant's offense conduct, the fact that he has the skill and expertise to develop and deploy computer viruses and other malicious software around the world, his demonstrated ability to amass and adapt hacking tools from open-source online platforms, his access to computers at home and at work once he returns to Italy, and his future proximity to co-conspirators also skilled in computer hacking (namely, Daniele Gasperini) after he returns to Italy, the government submits that the added measure of deterrence and protection provided by a one year term of supervised release is warranted here.

d. Forfeiture

The government also respectfully requests that the Court order forfeiture of the defendant's botnet, the defendant's infrastructure used to manage and run the botnet (including computers, command-and-control servers, and domains), and the defendant's backdoor (with username "request"). Title 18, United States Codes, Section 1030(i)(1)(A) requires that the Court, "in imposing sentence on any person convicted of a violation of this section . . . shall order, in addition to any other sentence imposed . . . that such person forfeit to the United States . . . such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation." As discussed above, the defendant used malicious software to install an unauthorized backdoor onto computer servers around the world and, in doing so, built a botnet that he used and intended to use in furtherance of his computer hacking and for fraud. That backdoor still exists on numerous computers around the world, whose true owners are unaware of its existence. Forfeiture of the botnet and the backdoor will permit the government to further identify the victims in this case, remediate the effects of the defendant's intrusions, and deny the defendant the ability to access his botnet or backdoor forevermore. The government will submit a proposed order of forfeiture for entry by the Court following sentencing.

V. Conclusion

The government respectfully requests that the Court impose a sentence of 12 months' imprisonment and a fine of $100,000. Given the seriousness of the defendant's conduct, such a sentence is sufficient, but not greater than necessary, to achieve Section 3553(a)'s purposes.

Respectfully submitted,

BRIDGET M. ROHDE
Acting United States Attorney

By: /s/
Saritha Komatireddy
Melody Wells
Assistant U.S. Attorneys
(718) 254-6054/6422

cc: Simone Bertollini, Esq. (by email and ECF)
Clerk of the Court (NGG) (by ECF)